APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **SECURE TERMINAL**

APPLICANT: **Michel LEGER**
Alain RHELIMI

"EXPRESS MAIL" Mailing Label Number: EV 710214849 US
Date of Deposit: June 19, 2006

SECURE TERMINAL

Technical field of the invention

This invention relates to secure terminals, for example, bank terminals or health terminals.

A bank terminal, connected to a telecommunication network, can carry out a bank transaction by the insertion of a bankcard with a magnetic strip or chip in the terminal, authentication of the cardholder, and entry of the nature and details of the transaction.

A health terminal, connected to a telecommunication network, allows analog access to medical or social security data relating to a holder of a health card with a magnetic strip and/or chip.

State of the prior technique

Figure 1 illustrates the functional diagram of a secure terminal TS, specifically banking, according to the previous design.

Such a terminal incorporates a group of functions, such as:

- a central processing unit 1 (micro-controller),
- a keypad 2,
- a volatile memory 3,
- a non-volatile memory 4,
- a display 5,
- a printer 6,
- an external connection interface 7,
- a magnetic card reader 8 and/or chip card reader 9,
- a means of connection to a telecommunication network 10, and
- a power supply unit 11 as energy (battery and/or mains).

These components are connected by a bus group 12 of different natures (power supply, memory, control) and are well known to the man skilled in the art. The whole is based on one or more printed circuits distributed in one or more boxes.

Implementation of this type of terminal is conventional other than that certain security elements must be added in order to proscribe all manipulations capable of altering or extracting financial information (personal identification number PIN, banking transactions, medical files, etc.).

For technical, financial and security reasons, the central unit (micro-controller), memories and certain peripherals for the input/output of sensitive data are confined to the same box. This box has an intrusion detector in order to guarantee the security of said box. Security remains principally physical for this type of solution.

In a more sophisticated embodiment, sensitive data, which moves via the buses and between the functional units, is encrypted. This mode is generally restricted to the central unit, which encodes this data [before sending it] to remote memories or assemblies via the modem.

Different configurations are possible.

A first configuration is a monolithic assembly, in which all the functional sub-assemblies are combined into a single box.

A second configuration is a bi-module assembly, in which the functional sub-assemblies are combined in two boxes according to two combinations. According to the first combination, all the sub-assemblies except the printer and the principal power supply are combined in a first box, and the printer and the power supply (for example the mains) are combined in a second box. According to the second combination, all the sub-assemblies except the principal power supply unit are combined in a first box, and the principal power supply unit (for example the mains) is found in a second box.

Only the second box, which contains the central unit and the peripherals for the input/output of sensitive data, is protected against intrusions.

Traditional solutions impose a global protection of the box and connect functions of different intellectual values. Thus, noble functions that are grouped around the central unit (memories and applications) are *de facto* connected to the same scale of value as the box that contains them.

Abstract of the invention

A first object of this invention is to reduce the cost of a secure terminal.
A second object of the invention is to improve the security of a secure terminal.
At least one of these objects is achieved by a secure terminal according to claim 1.

With the secure terminal of the new invention, the noble functions can be dissociated from those that are not.

The central unit, the memory, the applications and the data, together with the associated security for protecting these elements (for example the security module (SAM), the infraction detector, or the encryption device) have an important value within a secure terminal.

The ancillary peripherals such as the printer, the card reader [and] the modem have a low value. It will be the same for the power supply unit and the mechanics (box).

With the secure terminal of the new invention, the most valued part of the terminal is detached from the ancillary peripherals and concentrates the security efforts.

The secure terminal of the new invention thus exhibits advantages at the economic level and at the security level.

Brief description of the drawings

Other characteristics and advantages of the invention will appear in the following detailed but not exhaustive description of one embodiment and different alternatives, by reference to the appended drawings in which:

- figure 1, described already, represents schematically the functional elements of a secure terminal, in particular [for] banking, according to previous designs;
- figure 2 illustrates schematically the functional elements of a secure terminal, for banking in particular, according to the invention.

Detailed description of the invention

Figure 2 illustrates the functional breakdown of a secure banking terminal TS' according to the invention.

The value part is confined within a protected sub-assembly SEP that includes:

- a central unit 1,
- memories 3 and 4 in which data and applications are stored,
- a keypad 2, which is a delicate peripheral to be protected.
-

All of these components are interconnected by a conventional bus 12'.

According to one alternative, the display 5 can be a constitutional part of this protected sub-assembly SEP, in particular if the latter does not have a means of encryption.

According to another alternative, the display 5 can be a constitutional sub-assembly of the basic sub-assembly SEP constituting the part with low added value. According to this alternative, an encrypted communication can be set up with the display. In this case, the display has symmetrical or asymmetrical cryptographic means.

The basic sub-assembly SEB embodies:

- a printer 6,
- an external connection interface 7 (serial or parallel),

- a magnetic card reader 8 and/or a chip card reader 9,
- a means of connection to a telecommunication network such as a modem 10, and
- a power supply unit 11 as energy (battery and/or mains).

These components are interconnected by a conventional bus 12".

This protected sub-assembly is insertable, for example by means of a connector 13, in a basic sub-assembly SEB that is included in the part with low added value. The connector 13 is, for example, a connector of the PCMCIA type.

There is no need for this basic sub-assembly SEB to be certified.

The part(s) with low added value are combined in one or more boxes and one of them is intended to contain the valued and detachable sub-assembly SEP.

The protected sub-assembly SEP incorporates:
- the applications,
- the electronic architecture of the heart of the terminal,
- the means providing the security (for example the SAM module, etc.).

The protected sub-assembly SEP constitutes a detachable module, easily distributable and capable of being integrated into a bank terminal by the same manufacturer or by a third party (OEM "Original Equipment Manufacturer or ODM "Original Design Manufacturer").

The protected sub-assembly SEP constitutes a sealed module, for example, impossible to remove without destruction. It can be certified. It contains the keypad used to enter sensitive data. The connection between the keypad 2 and the microcontroller 1 of the protected sub-assembly SEP proscribes any repair but permits the use of non-secure components. Therefore the protected sub-assembly SEP can be manufactured from standard components, comprising in particular a standard keypad, the securing of which

is simple and economical. The level of security achieved is that traditionally termed "detection of evident fraud" (or "evident tamper").

The solution provided by the invention can also resolve problems of migration and maintenance.

Simple migration for a client from a former generation terminal to a new generation [terminal] exhibiting improved features (for example new printer, colour display, new modem (WIFI or ADSL). With the protected sub-assembly SEP, the data is transferred in total security and instantaneously to a new reception platform (basic sub-assembly SEB).

Maintenance is simplified in the event of a breakdown of the basic sub-assembly SEB as it suffices to detach the protected sub-assembly SEP and install it in a new basic sub-assembly SEB.

With the invention, it is possible to normalise the dimensions and/or the connector technology of the protected sub-assembly SEP in order to allow simplified migration for the terminal manufacturer. Indeed, the latter can change the architecture and technology of the protected sub-assembly SEP according to the opportunities offered by the market.

Maintenance of the protected sub-assembly SEP is simplified as the latter is sealed and is therefore disposable. By construction, the latter cannot be removed without destroying it.

Finally, from the point of view of the user, it is possible to share a basic sub-assembly SEB with several protected sub-assemblies SEP connected to different users (hypermarket, open market, etc.), the protected sub-assembly SEP thus fulfilling the task of "box" for personal and secure data.